

**IN THE CLAIMS**

Claims 5, 17 and 29 are amended.

1 1. (Cancelled)

1 2. (Cancelled)

1 3. (Cancelled)

1 4. (Cancelled)

Sub EI  
1 5. (Currently Amended) A computer-implemented system for protecting a  
2 network, comprising:  
3 a vulnerability detection system (VDS) for gathering information about the  
4 network to determine vulnerabilities of a plurality of hosts on the  
5 network; and  
6 an intrusion detection system (IDS), cooperative with the VDS, for examining  
7 network traffic responsive to the vulnerabilities of a host from the  
8 plurality of hosts as determined by the VDS to detect traffic indicative  
9 of malicious activity.

DI  
1 6. (Previously Presented) The system of claim 5, wherein the VDS is  
2 adapted to gather information about the network by sending data to the plurality of hosts  
3 and receiving responsive data from the plurality of hosts.

1 7. (Previously Presented) The system of claim 6, wherein the VDS is  
2 adapted to gather information automatically provided by the plurality of hosts.

1 8. (Previously Presented) The system of claim 7, further comprising:  
2 a vulnerabilities rules database, in communication with the VDS, for storing  
3 rules describing vulnerabilities of the plurality of hosts,

4 wherein the VDS is adapted to analyze the gathered information with the rules  
5 to determine the vulnerabilities of the plurality of hosts.

1 <sup>5</sup> ~~9.~~ (Previously Presented) The system of claim <sup>4</sup> ~~8~~, wherein the VDS is  
2 adapted to analyze the gathered information with the rules to identify operating systems  
3 on the plurality of hosts and determine the vulnerabilities responsive to the respective  
4 operating systems.

1 <sup>6</sup> ~~10.~~ (Previously Presented) The system of claim <sup>4</sup> ~~8~~, wherein the VDS is  
2 adapted to analyze the gathered information with the rules to identify open ports on the  
3 plurality of hosts and determine the vulnerabilities based on the open ports.

1 <sup>7</sup> ~~11.~~ (Previously Presented) The system of claim <sup>4</sup> ~~8~~, wherein the VDS is  
2 adapted to analyze the gathered information with the rules to identify applications  
3 executing on the plurality of hosts and determine the vulnerabilities based on the  
4 applications.

1 <sup>8</sup> ~~12.~~ (Original) The system of claim <sup>1</sup> ~~5~~, further comprising:  
2 an intrusion rules database, in communication with the IDS, for storing rules  
3 describing malicious activity,  
4 wherein the IDS is adapted to analyze the network traffic with the rules to  
5 detect network traffic indicative of exploitations of the determined  
6 vulnerabilities.

1 <sup>9</sup> ~~13.~~ (Original) The system of claim <sup>1</sup> ~~8~~, wherein the IDS is adapted to detect  
2 traffic indicative of exploitations of only the determined vulnerabilities.

1 <sup>10</sup> ~~14.~~ (Cancelled)

1 <sup>10</sup> ~~15.~~ (Original) The system of claim <sup>1</sup> ~~8~~, wherein the VDS is adapted to update  
2 the determined vulnerabilities, and wherein the IDS is adapted to detect traffic indicative  
3 of malicious activity in response to the update.

11  
10  
1 16. (Original) The system of claim 15, wherein the VDS is adapted to update  
2 the determined vulnerabilities in response to a change in the network.

Sub E2  
1 17. (Currently Amended) A computer-implemented method for protecting a  
2 network, comprising:  
3 gathering information about the network to determine vulnerabilities of a  
4 plurality of hosts on the network; and  
5 cooperative with the step of gathering information examining network traffic  
6 responsive to the determined vulnerabilities of a host from the plurality  
7 of hosts to detect network traffic indicative of malicious activity.

13  
1 18. (Previously Presented) The method of claim 17, wherein gathering  
2 information comprises sending data to plurality of hosts on the network and receiving  
3 responsive data from the plurality of hosts.

D1  
14  
1 19. (Previously Presented) The method of claim 17, wherein gathering  
2 information comprises receiving data automatically provided by the plurality of hosts on  
3 the network.

15  
1 20. (Previously Presented) The method of claim 17, further comprising:  
2 storing rules to describe vulnerabilities of the plurality of hosts,  
3 wherein determining vulnerabilities includes analyzing the gathered  
4 information with the rules.

16  
1 21. (Previously Presented) The method of claim 20, wherein determining  
2 vulnerabilities comprises analyzing the gathered information with the rules to identify  
3 operating systems on the plurality of hosts.

17  
1 22. (Previously Presented) The method of claim 20, wherein determining  
2 vulnerabilities comprises analyzing the gathered information with the rules to identify  
3 open ports on the plurality of hosts.

1 <sup>18</sup>~~23.~~ (Previously Presented) The method of claim <sup>15</sup>~~20~~, wherein determining  
2 vulnerabilities comprises comparing the gathered information against the rules to identify  
3 applications on the plurality of hosts.

1 <sup>14</sup>~~24.~~ (Original) The method of claim <sup>12</sup>~~17~~, further comprising:  
2 storing rules describing malicious activity,  
3 wherein detecting network traffic indicative of malicious activity comprises  
4 analyzing the network traffic with the rules to detect traffic indicative  
5 of exploitations of the determined vulnerabilities.

1 <sup>20</sup>~~25.~~ (Original) The method of claim <sup>12</sup>~~17~~, wherein examining network traffic  
2 consists of detecting traffic indicative of exploitations of only the determined  
3 vulnerabilities.

1 <sup>D</sup> ~~26.~~ (Cancelled)

1 <sup>24</sup>~~27.~~ (Previously Presented) The method of claim <sup>12</sup>~~17~~, further comprising:  
2 updating the determined vulnerabilities and detecting traffic indicative of  
3 malicious activity in response to the update.

1 <sup>22</sup>~~28.~~ (Original) The method of claim <sup>21</sup>~~27~~, wherein the updating is responsive to a  
2 change in the network.

Sub  
E3  
1 ~~29.~~ (Currently Amended) A computer program product, comprising:  
2 a computer-readable medium having computer program logic embodied  
3 therein for protecting a network, the computer program logic:  
4 gathering information about the network to determine vulnerabilities of a  
5 plurality of hosts on the network; and  
6 cooperative with the step of gathering information, examining network traffic  
7 responsive to the determined vulnerabilities of a host from the plurality  
8 of hosts to detect network traffic indicative of malicious activity.

1 <sup>24</sup>  
2 ~~30.~~ (Previously Presented) The computer program product of claim <sup>23</sup>~~29~~,  
3 wherein gathering information comprises sending data to plurality of hosts on the  
network and receiving responsive data from the plurality of hosts.

1 <sup>25</sup>  
2 ~~31.~~ (Previously Presented) The computer program product of claim <sup>23</sup>~~29~~,  
3 wherein gathering information comprises receiving data automatically provided by the  
plurality of hosts on the network.

1 <sup>26</sup>  
2 ~~32.~~ (Previously Presented) The computer program product of claim <sup>23</sup>~~29~~,  
3 further comprising:  
4 storing rules to describe vulnerabilities of the plurality of hosts,  
5 wherein determining vulnerabilities includes analyzing the gathered  
information with the rules.

D1  
1 <sup>27</sup>  
2 ~~33.~~ (Previously Presented) The computer program product of claim <sup>24</sup>~~32~~,  
3 wherein determining vulnerabilities comprises analyzing the gathered information with  
the rules to identify operating systems on the plurality of hosts.

1 <sup>28</sup>  
2 ~~34.~~ (Previously Presented) The computer program product of claim <sup>26</sup>~~33~~,  
3 wherein determining vulnerabilities comprises analyzing the gathered information with  
the rules to identify open ports on the plurality of hosts.

1 <sup>29</sup>  
2 ~~35.~~ (Previously Presented) The computer program product of claim <sup>26</sup>~~34~~,  
3 wherein determining vulnerabilities comprises comparing the gathered information  
against the rules to identify applications on the plurality of hosts.

1 <sup>30</sup>  
2 ~~36.~~ (Original) The computer program product of claim <sup>23</sup>~~35~~, further comprising:  
3 storing rules describing malicious activity,  
4 wherein detecting network traffic indicative of malicious activity comprises  
5 analyzing the network traffic with the rules to detect traffic indicative  
of exploitations of the determined vulnerabilities.

23

31  
1 ~~31~~. (Original) The computer program product of claim ~~29~~, wherein examining  
2 network traffic consists of detecting traffic indicative of exploitations of only the verified  
3 vulnerabilities.

D1  
1 ~~38~~. (Cancelled)  
2 ~~32~~  
1 ~~39~~. (Previously Presented) The computer program product of claim ~~29~~<sup>23</sup>, further  
2 comprising:  
3 updating the determined vulnerabilities; and  
4 detecting traffic indicative of malicious activity in response to the update.

33  
1 ~~40~~. (Previously Presented) The computer program product of claim ~~39~~<sup>32</sup>,  
2 wherein the updating is responsive to a change in the network.